IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 9, 2020, accepted February 23, 2020, date of publication February 28, 2020, date of current version March 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2977048

Public Auditing Scheme With Identity Privacy Preserving Based on Certificateless Ring Signature for Wireless Body Area Networks

KAIXIN ZHAO, DONG SUN, GANG REN, AND YANG ZHANG
College of Computer Science and Technology, Henan Institute of Technology, Xinxiang 453003, China
Corresponding author: Kaixin Zhao (zhaokx_2008@126.com)

This work was supported by the Key Technologies Research and Development Program of Henan Province under Grant 202102210153, Grant 192102210113, and Grant 192102210248.

ABSTRACT The emergence of Wireless Body Area Networks (WBAN) provides users with ubiquitous wireless communication services, such as continuous exchange of medical information in real time. Therefore, WBAN is considered to be one of the effective wireless sensor technologies for improving medical services. However, the characteristics of WBAN make it subject to multiple attacks, such as the leakage of private information of users, and WBAN is also inefficient. In this paper, a certificateless ring signature scheme CLRS is proposed. In addition, we propose a public auditing scheme with identity privacy protection, which combines the certificateless ring signature technology for cloud-assisted body area network. Through the analysis of security, it shows that the scheme can resist the existing attack methods such as forging attacks. Finally, the comparison between theoretical analysis and experimental simulation shows that the scheme has obvious efficiency advantages compared with the existing scheme.

INDEX TERMS Public auditing, privacy preserving, certificateless ring signature, wireless body area networks.

I. INTRODUCTION

The body area network (BAN) was first proposed by Zimmerman [1] in 1996, which is also called of the wireless body area network (WBAN) because of the use of wireless communication technology. The wireless body area network is a network in the 3-5 meter range of the human body. Generally speaking, wireless body area network devices can be divided into wearable devices and implanted devices: wearable devices can be deployed on the human body surface or clothing, and implanted devices can be implanted into the human body. These sensors can continuously detect physiological parameters such as electrocardiogram, electroencephalogram, blood pressure, pulse and so on, and transmit the collected physiological information to gateway or controller through WiFi or Bluetooth wireless communication technology. The controller can locally store or analyze the collected physiological data, or transmit it to the medical application system such as the remote medical server or cloud service platform through external network, so as to provide health recommendations. The medical staff can also diagnose and deal with the patient's sudden disease in time.

From the aspect of network architecture, the wireless body area network can be divided into three layers: the sensing layer, the transmission layer and the application layer, the structure model is shown in Figure 1. The sensing layer is composed of a series of biosensors, which are mainly responsible for the collection of body blood glucose, blood pressure, ECG, EEG and other physiological signals, and transmits data [2] through the micro wireless module carried by itself. The transport layer, also known as the network layer, is mainly used for data exchange and transfer links. Due to the deployment around the human body, considering the convenience of deployment, the wireless communication technology is usually used for communication. In the transport layer, Hub needs to be a forwarding device to forward the physiological data collected by the sensor nodes. The application layer includes various types of medical application servers. After receiving the physiological data transmitted by Hub, the medical application server analyzes and processes

The associate editor coordinating the review of this manuscript and approving it for publication was Maode Ma.

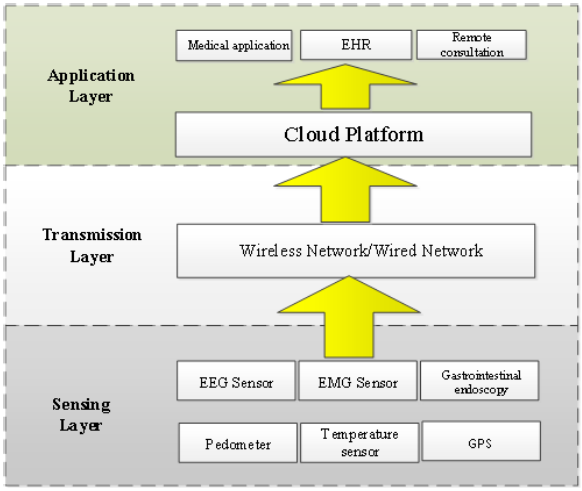

FIGURE 1. The three layers of WBAN.

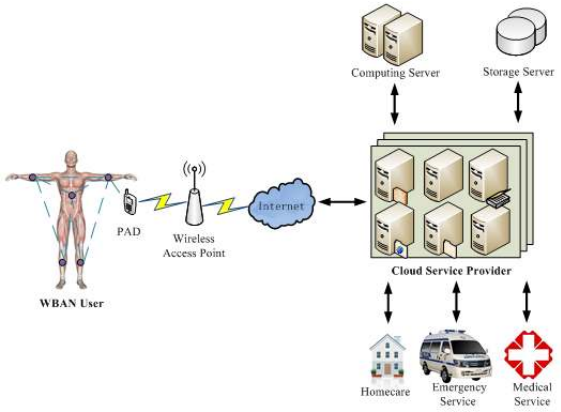

FIGURE 2. The system model of cloud-assisted body area network.

the analysis results, and sends the analysis results to the doctor or user [3], [4].

In view of the great effect of wireless body area network technology on reality, many research institutions at home and abroad have carried out research on wireless body area network technology [5]–[8]. In 2004, Harvard University has developed a CodeBlue system for emergency [6]; the same year, the French CENS launched MARSIAN [7], MARSIAN is a wrist joint dynamic monitoring and recording system (Intelligent gloves embedded with physiological sensor) for the detection of autonomic nervous system activity; in 2005, NASA and Stanford University jointly developed the Life-Guard [8] rescue system for space and terrestrial applications.

At 2012, Giancarlo Fortino et al. proposed the concept of ''BodyCloud'' for the first time at CloudCom conference [9], which is combining the body area network with cloud computing firstly (as Figure 2 shown). Giancarlo Fortino et al. believe that the combination of resource constrained body area network with the massive and flexible cloud computing technology will provide users with more services, and elaborate the four reasons for the combination of WBAN and cloud services.

A. MANAGEMENT

the data in the body area network involves how to collect, manage, store and transmit effectively. Multiple body sensors get data sources in real time and the related activities that may be distributed in time or space. Time distribution refers to the activities carried out at different times and harmonize the effect. Spatial distribution means that activities may be distributed at different locations, while data networks are connected together. Cloud computing infrastructure can facilitate these data management functions and storage.

B. PROCESSING

data collected from somatic nodes are processed into physical quantities, and are combined into other forms of data, for example, combining body temperature reading with blood pressure readings into patients' health charts. In the presence of multiple input data streams from the body area network, data processing is the necessary operation for making critical decisions in real time, and this operation may be computationally intensive. The cloud infrastructure can provide a wealth of computing resources.

C. SERVICE INVOCATION

the problem of how the data collected from the network is processed and how to be allocated. The process is executed by automatically forming the workflow and invoking services. This operation process requires a platform such as cloud infrastructure to support automatic workflow formation.

D. DATA ANALYSIS

the somatic data that is introduced into various analysis and modeling tools can be further used in various applications and decision-making systems. Analysis operations rely on appropriate storage and middleware technologies to perform high and fast data processing. It can take advantage of the ability of cloud processing and provide fast response.

After Giancarlo Fortino proposed the concept of ''BodyCloud'', many scholars have studied the architecture of cloud-assisted body area network. In 2013, Wan et al. put forward a pervasive health application framework [10] combined with wireless body area network and mobile cloud computing technology, and proposed energy efficient routing strategy, cloud resource allocation and heterogeneous cloud-assisted somatic network semantic interoperability and other solutions. In 2017, in literature [11], Chen et al. based on intelligent wearable devices, combined with edge computing and cloud computing technology, put forward the concept of ''Wearable 2'' to enhance the next generation of health care system QoS (quality of service) and QoE (experience quality). To evaluate the feasibility of the network, in the same year, Yu et al. from the Chinese University of Hong Kong [12] did the simulation test of the 24 hour operation of the cloud assisted body sensor network and the support of the

concurrent users. In 2018, Yu *et al.* [12] designed a new architecture for the emergency healthcare system based on mobile cloud computation (MCC) and fifth-generation (5G) wireless link is proposed. Based on the processing speed of MCC and the communication rate of 5G scheme, this system can monitor and locate patients in real time.

Although the combination of resource constrained body area network with clouds with massive and flexible capacity, it provides more rich digital services for users. However, the introduction of cloud server has brought new security and privacy risks, cloud-assisted body area network data is used in the diagnosis of disease of the user, so there are strict requirements for the correctness of the data, and how to detect the data stored in the cloud server is correct, needs a suitable remote data integrity checking mechanism for cloud-assisted body area network. And the public auditing scheme can be used to solve this problem.

However, in the existing public auditing schemes, the third party auditor needs to get the user's public key information, but the user's public key is one-to-one correspondence with the user's identity, so it will expose the user's identity privacy. In wireless body area network applications, data related to user's health information is very sensitive. Through the third party auditor will complete the auditing work with cloud server faithfully, but as a semi-trusted entity, it still may get user's identity privacy information. How to ensure that cloud servers and auditors provide users with services at the same time and do not disclose patient's identity privacy has become one of the hot issues in this area.

At present, there are many public auditing schemes for privacy protection have been put forward [14]–[20]. These schemes can be divided into two categories, one kind is data content privacy protection [14]–[16], and the other kind is user identity privacy protection [17]–[20], [29]. The data content privacy protection is considering how to audit the data while allowing the third party auditors can not obtain any information about the storage of data; the identity privacy mainly considers how to make the auditing task and does not retrieve any identity information of the data owner. At present, there are only few researches have covered the identity privacy protection problem, such as schemes with ring signature [17]–[19], group signature [20], [29]–[32]. However, these public auditing schemes with privacy protection have high computational cost. The cloud-assisted body area network is resource–constrained, therefore, it is of great significance to propose an efficient and practical public auditing scheme with identity privacy preserving for cloud-assisted body area network.

II. PUBLIC AUDITING SCHEME WITH IDENTITY PRIVACY PRESERVING

Based on the above discussions, in this paper, a certificateless ring signature scheme CLRS is proposed firstly. Next, based on CLRS, a public auditing scheme with identity preserving is put forwarded and be applied to cloud-assisted body area network environment. Based on this scheme, when cloud servers and auditors provide storage and audit services for WBAN applications such as hospitals, they can only be sure that the data is derived from an anonymous group but not a certain individual, thereby protecting users' identity privacy.

TABLE 1. The efficiency comparison of ring signature schemes.

Scheme	Signature length	Signing operations	Verifying operations
Herranz–Saez [21]	$(2n+1)\|Z^p\|$	$(2n-1)SM$	$(n+1)SM$
Boneh et al. [22]	$n\|G_1\|$	$(2n+1)SM$	$(n+1)P$
Zhang et al. (ZSS) [23]	$n\|G_1\|$	$(2n-1)SM$	$(n+1)P$
Shacham–Waters [24]	$(2n+1)\|G_n\|$	$(3n+2)SM$	$(2n+3)P_N$
Schage–Schwenk [25]	$(n+1)\|G_1\|$	$(2n+1)SM$	$(n+2)P$
Liu–Yuen–Zhou [26]	$(2n+3)\|G_n\|$	$(3n+4)SM$	$(2n+5)P_N$
RSCP [27]	$n\|G_1\|+\|G_2\|$	$(n+1)SM$	$2P+nSM$

In the process of designing the certificateless ring signature scheme in this section, the ring signature scheme RSCP designed by Shim [27] is improved and a certificateless version is constructed. Here we use the RSCP scheme designed by Shim et al. is due to the high efficiency of the scheme. Table 1 lists the efficiency comparison between the RSCP and other ring signature schemes. It can be found that the RSCP scheme is better than other schemes no matter in the length of signature, or in the computation complexity of signature and verification. In the next section, we will introduce the certificateless ring signature scheme CLRS and public auditing scheme with identity privacy protection for cloud-assisted wireless body area network based on CLRS.

A. THE SYSTEM MODEL FOR PUBLIC AUDITING SCHEME WITH IDENTITY PRIVACY PRESERVING

There are four roles in our scheme including of:cloud server, key generate center, auditor and user.

1) CLOUD SERVER

cloud server is a semi-trusted entity with large capacity of computational and storage resources;user uploads the data collected with sensors to cloud server to save the storage cost locally. Considering that the cloud server is semi-trusted, although it will fulfill the whole protocol process, it may make unauthorized access to user sensitive privacy data.

2) KEY GENERATE CENTER (KGC)

the KGC is specially responsible for generating the public parameters of the system and generating the partial public key/partial private key for each role. The key center is a semi-trusted entity. Third Party Auditor: the third party auditor is a semi-trusted entity and is responsible for the integrity testing task. When the user wants to check whether data stored in the remote cloud server is correct, the user request to the third party auditor, third party audit server sends the challenge information to the cloud server and receives the response information: auditing proof. Based on the auditing proof, third party auditors can test data integrity and test results will be sent to the data owner.

3) USER

the user is a cloud-assisted wireless body area network service user. Users use the sensors to collect physiological data on the body and upload to the cloud server to construct user physiological data record; before uploading, user needs to generate the tags for the using of integrity checking; for the reason that the data stored in the cloud server is privacy physiological data, so user wants to be anonymous when auditing data in order to protect users identity privacy.

B. SECURITY REQUIREMENTS

In addition to realize public auditing of remote data, our scheme should also be able to achieve the purpose of protecting user's identity privacy. Below is a list of the design goals to be met in the designing of this scheme:

1) PUBLICLY VERIFIABLE

third party auditors can verify whether the data stored on cloud servers are well stored without having to download all stored data and impose additional computational burden on users.

2) STORAGE CORRECTNESS

only the cloud server that stores the data owner's data can verify the integrity of the data with an interactive protocol with the third party auditor.

3) IDENTITY PRIVACY PROTECTION

in the process of uploading and auditing, the auditor can not obtain the corresponding information of any auditing data and the identity of the data owner.

4) BATCH AUDITING

when receiving testing requests of multiple data blocks, the third party auditor should be able to simultaneously detect multiple data blocks for one-time, thereby improving the efficiency of the system.

C. CLRS CERTIFICATELESS RING SIGNATURE SCHEME

In this section, the design of the certificateless ring signature scheme CLRS will be introduced. The CLRS scheme in this section includes of five polynomial time algorithms: system setup, partial-key generation, user key generation, signature and verification. The system setup process is used to generate public parameters, the system master key and the public key. The master key is mainly used when receiving partial key generating user request, embedding the personal information and the master key into the user's partial key. So ''trusted factors'' will be embedded into the signature when user use partial key to generate signature for message; after receiving a signature, the public key and the user can use the corresponding public key to verify the validity of the signature, the public key system is a ''credible information'', this parameter shows that the signature or the private key has been authorized by the key generation center, which will be different with the PKI system and save the cost of certificate storage and transmission. But because of the inherent nature of the ring signature, in the process of signature verification, a large number of public key user needs to be used, if we use the certificate-based scheme, then a large number of certificates transmission and storage costs are consumed, and the wireless body area network is an especially resource constrained environment, it will greatly be a burden of storage and communication to the system; although the identity-based schemes do not needs certificate, but due to key escrow problem that key center authority is too high, will cause the system in high security risks.

TABLE 2. Notations list for CLRS.

Symbol	Description
U_i	User$i$
G_1	A multiplicative group G_1 with order q
G_2	A multiplicative group G_2 with order q
P	Random element on G_1
Q	Random element on G_2
PK_Z	The public key of user Z
$SK_{Z,1}$	The partial key of user Z generated by KGC
$SK_{Z,2}$	The partial key of user Z generated by user
E	Bilinear pairing $G_1 \times G_1 \rightarrow G_2$
H_2	A one-way hash function $G_1 MG_1^n \rightarrow Z_q^*$
Msk	The master key of KGC
P_{pub}	The public key of KGC
H_1	Hash function: $\{(0,1)^*, G_1, G_1, G_1\} \rightarrow Z_q^*$
H_1	Hash to point function:$\{(0,1)^*, G_1\} \rightarrow G_1$

In the certificateless system, the user generate the private/public key to themself, and the user's private key is combined with the key generated in this part and the other partial key extracted by key generation center in the partial key extraction phase; in the process of the signing algorithm, the user collects the other users' public key, calls this algorithm to sign a message to generate an anonymous signature (ring signature), signature receiver can use verification algorithm to verify the signer's signature, verification algorithm requires the user to input the signers' public key and key center's public key; in the verification process, the verifier only knows the signer comes from these users but do not know the specific information, so as to protect the identity of user's privacy. In this paper, based on the Shim's ring signature scheme RSCP, a certificateless ring signature scheme CLRS is designed. The following is the introduction of the certificateless ring signature scheme, CLRS, which is built in this paper. Table 2 lists the symbols used in the CLRS scheme.

1) SYSTEM SETUP

Algorithm 1 defines the system setup phase of our certificateless ring signature scheme which inputs a security parameters 1 and outputs the public parameters $(q, G_1, G_2, P, H, h, e, PK_{KGC})$.

2) PARTIAL-KEY EXTRACTION

Similar to certificateless signature scheme, new users need to apply for the KGC to compute a partial key. The process is as follows:

The user sends a request to the key center with own identity information ID_i, the KGC computes $SK_{i,1} = hID_i) \cdot msk \cdot P$.

Algorithm 1 System Setup

Input: security parameters l
Output: public parameters $(q, G_1, G_2, P, H, h, e, P_{pub})$
1)KGC generate a large prime number q satisfying: $q > 2^l$;
2)KGC chooses the parameters below:
3) $<G_1, \cdot >$; // the cyclic multiplicative group with order q;
4) $<G_2, \cdot >$; // the cyclic multiplicative group with order q;
5) $P \in G_1$ //the generator in G_1;
6) $Q \in G_2$ // the generator in G_2;
7) KGC chooses a bilinear pairing function $e : G_1 \times G_2 \rightarrow G_T$;
8) KGC chooses a one-way hash function $G_1 MG_1^n \rightarrow Z_q^*$;
9) Chooses a random number $msk \in Z_q^*$;//generate the system master key
10)Compute $P_{pub} = msk \cdot Q$;//generate the system public key;
11)returns$\{G_1, G_2, P, Q, e, q, H, P_{pub}\}$;

3) USER-KEY GENERATION

After applying for the partial key, the user selects the user's key. The specific process is as follows:

For user U_i, selects a random number $s_i \in Z_q^*$ and sets $SK_{i2} = s_i$. Compute the corresponding user's public key $PK_i = s_i \cdot P$. After this phase, set user's secret key as $SK_i = \{SK_{i1} SK_{i2}\}$, public key as PK_i.

After all the key establishment has been completed, the user calls the algorithm 2 to sign the message $m \in \{0, 1\}^*$. Before signing, the signer collects the other n users' public key and constructs public key sets $\{PK_1, PK_2, \cdots, PK_n\}$. Then input the public key sets $\{PK_1, PK_2, \cdots, PK_n\}$, signer's secret key SK_i message $m \in \{0, 1\}^*$ into algorithm 2 and gets the ring signature $S = \{A_1, A_2, \ldots, A_n, B, O\}$.

When the signature receiver receives the message and the corresponding signature, the algorithm 3 can be invoked to verify the signature. The verification process requires the input of the public key sets $\{PK_1, PK_2, \cdots, PK_n\}$, $m \in \{0, 1\}^*$ and KGC's public key P_{pub}. Finally, calling the algorithm 3 and returns the verification result "TRUE" or "FALSE". "TRUE" represents that the signature passes the verification, and "FALSE" represents the signature on message is illegal. It should be noted that in the process, the verifier can not get the specific identity information of the signer, and the verifier only knows that the signer is a member comes from the group of public key set $\{PK_1, PK_2, \cdots, PK_n\}$ and do not know which one is the specific member.

D. THE PUBLIC AUDITING SCHEME WITH IDENTITY PRIVACY PRESERVING BASED ON CLRS

In this section, a public auditing scheme with identity privacy preserving is proposed, based on the certificateless ring signature scheme CLRS which is proposed in the previous section. In our scheme, based on the anonymity of ring signature, auditors will not get the data owner's identity information in the process of integrity checking; in addition, because of the solution is based on certificateless technology, greatly reducing the user's storage and communication costs in the body area network environment with limited resources. There are six algorithms in our scheme: system setup, partial key generation, user key generation, tags generation, proof generation and verification. Figure 3 is a diagram of the system model of our privacy protection auditing scheme proposed in this paper, and table 3 lists the symbols used in this section.

Algorithm 2 Ring Signature

Input: public key sets $\{PK_1, PK_2, \cdots, PK_n\}$, signer's secret key SK_i, message $m \in \{0, 1\}^*$
Output: ring signature $S = \{A_1, A_2, \ldots, A_n, B, O\}$
1)*for*$(i = 1; (i <= n) \&\& (i \neq j); i++)$
2){
3) chooses:
4) $A_i \in G_1$;
5)} //end for, chooses $n-1$ elements in G_1
6)*for*$(i = 1; i <= n; i++)$
7){
8) Computes:
9) $h_i = H(A_i, m, PK_1, PK_2, \cdots, PK_n)$;
10)}//end for
11)*for*$(i = 1; (i <= n) \&\& (i \neq j); i++)$
12){
13) Chooses: $r, t \in Z_q^*$;
14) computes:
15) $A_j = t \cdot P + r \cdot SK_{i1} - \sum_{i \neq j}^{n} (h_i \cdot PK_i + A_i)$;
16) $B = (t + h_j \cdot SK_{i2}) \cdot Q$;
17) $O = r \cdot hID_i)$;
18)} //end for, compute ring signature
Returns $S = \{A_1, A_2, \ldots, A_n, B, O\}$

Algorithm 3 Signature Verification

Input: public key sets $\{PK_1, PK_2, \cdots, PK_n\}$, message $m \in \{0, 1\}^*$, P_{pub}
Output: "TRUE" or "FALSE"
1)*for*$(i = 0; i <= n; i++)$
2){
3) Computes: $h_i = H(A_i, m, PK_1, PK_2, \cdots, PK_n)$
4) }//end for
5)Verify the equation

$$e\left(P, B + O \cdot P_{pub}\right) = e\left(\sum_{i=1}^{n} (h_i \cdot PK_i + A_i), Q\right);$$

//check the signature
6)Returns "TRUE"or "FALSE"

1) SYSTEM SETUP

similar to algorithm 1, KGC generates two cyclic multiplicative group G_1, G_2 with order q, a bilinear pairing $e : G_1 \times G_2 \rightarrow G_T$ and a one-way hash function $H : \{0, 1\}^* \rightarrow G_1$.

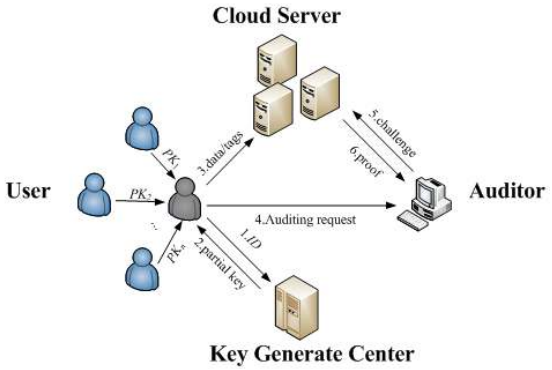

FIGURE 3. The system model of our privacy preserving storage auditing scheme for cloud-assisted WBAN.

TABLE 3. Notations list for public auditing scheme with identity privacy preserving.

Symbol	Description
U_i	User
G_1	An cyclic multiplicative group G_1 with order q
G_2	An cyclic multiplicative group G_2 with order q
P	Generator of G_1
Q	Generator of G_2
PK_Z	the public key of user Z
$SK_{Z,1}$	the partial key of user Z generated by KGC
$SK_{Z,2}$	the partial key of user Z generated by user
E	a bilinear pairing $G_1 \times G_1 \rightarrow G_2$
H	A one-way hash function $G_1 MG_1^n \rightarrow Z_q^*$
Msk	the system's master key
P_{pub}	System public key
c_i/m_i	The user's medical data m_i and corresponding cypher text c_i
$Chal$	The challenge information of auditor $Chal = \{(i, r_i)\}_{i \in I}$

Chooses two random elements $P \in G_1$, $Q \in G_2$. Finally KGC chooses a random number $msk \in Z_q^*$ as system master key and computes $P_{pub} = msk \cdot Q$, KGC public system public parameters:$\{G_1, G_2, P, Q, e, q, H, P_{pub}\}$.

2) PARTIAL KEY GENERATION

before cloud-assisted body area network users access the system, they need to send their own identity information ID_i to KGC, KGC computes $SK_{i1} = HID_i) \cdot msk \cdot P$ for new user to generate partial key.

3) USER KEY GENERATION

for user U_i, choose a random number $s_i \in Z_q{}^*$ and sets $SK_{i2} = s_i$, calculate the user's public key $PK_i = s_i \cdot P$. After the user's key generation phase is completed, set user's private key as $SK_i = \{SK_{i1} SK_{i2}\}$, and the user's public key as PK_i. All the key generation operations are completed by the above steps.

4) TAGS GENERATION

when the user wants to upload the data collected by the sensors to the server, the data files need to be partitioned. Here, suppose the data file has k block, the user collects the public key of the other users and gets the key set $\{PK_1, PK_2, \cdots, PK_n\}$. Given a set of public key, $\{PK_1, PK_2, \cdots, PK_n\}$, user's private key SK_s, for a message $m_i \in \{0, 1\}^*(i \in [1, n])$ the tag is calculated as follows:

Algorithm 4 Tag Generation

Input: security parameter l
Output: tag $S = \{A_{i,1}, A_{i,2}, \ldots, A_{i,n}, B_i\}$
1)$for(j = 0; (j <= n)\&\&(j \neq s); j++)$
2){
3) Chooses: $A_{i,j} \in G_1$; //chooses $n-1$ elements in G_1;
4) }//end for
5)chooses: $o, t \in Z_q^*$
6)computes:
7) $A_j = t \cdot P + r \cdot SK_{i1} - \sum_{i \neq j}^{n} (h_i \cdot PK_i + A_i)$;
8) $B = (t + h_j \cdot SK_{i2}) \cdot Q$;
9) $O = r \cdot hID_i)$;
10) returns $S = \{A_{i,1}, A_{i,2}, \cdots, A_{i,n}, B_i, O\}$

After the completion of algorithm 4, the user uploads the data $\{m_1, m_2, \cdots, m_n\}$ and the corresponding tags to the cloud server. The cloud server stores the data and the corresponding tags.

5) PROOF GENERATION

if the user wants to detect whether the data stored at the cloud server is correctly saved, the user sends the checking request to the auditor, and the auditor performs an interactive algorithm 5 with the cloud server, generates proof (Pro, C) and return it to the auditor.

Algorithm 5 Proof Generation

Input: $S = \{A_{i,1}, A_{i,2}, \ldots, A_{i,n}, B_i\}$
Output: (Pro, C)
1)The third part auditor generates the tuple $Chal = \{(i, r_i)\}_{i \in I}$, I is an i-elements sets and $i \in [1, n]$, $r_i \in Z_q^*$; //generates the challenge message
2)The third part auditor sends $Chal$ to cloud server; //sends challenge message
3)Cloud server computes:
4) $A_1 = \sum_{j=1}^{c} r_j \cdot A_{j,1}$;
5) $A_2 = \sum_{j=1}^{c} r_j \cdot A_{j,2}$;
6) $\cdots$
7) $A_n = \sum_{j=1}^{c} r_j \cdot A_{j,n}$;
8) $M = \sum_{j=1}^{c} r_j \cdot m_j$;
9) $B = \sum_{j=1}^{c} r_j \cdot B_j$;
10) Returns $(A_1, A_2, \cdots, A_n, M, B)$

Proof verification: This is the last stage of the whole scheme, after the auditor received proof (Pro, C), checks if

the equation $e(P, B + O \cdot P_{pub}) = e(\sum_{i=1}^{n} (M \cdot PK_i + A_i), Q)$ is hold, results are returned as a Boolean value: "TRUE" represents that the detected data stored properly, "FALSE" represents the existence of incorrect data block storage. Finally, the auditor returns the results to the user. So far, all the algorithms of the scheme are finished. In the next section, we will analyze the security of the scheme by means of the formal proof method under the random oracle model, and analyze the efficiency of the scheme through simulation experiments.

III. THE SECURITY ANALYSIS OF PUBLIC AUDITING SCHEME WITH IDENTITY PRIVACY PRESERVING

In this section, we will analyze the security of our scheme. There are two parts respectively. The first part is non-formal analysis of the security goals achieved by the scheme. In the non-formal analysis basis, by deriving formal proof in the random oracle model to prove the unforgeability of our scheme, the security assumption of the certificateless ring signature scheme and the identity privacy public audit scheme is based on the co-CDH problem. If the co-CDH's difficult assumption is hold, the scheme can not be overcomed by a polynomial time attacker.

A. SECURITY GOALS ANALYSIS

1) IDENTITY PRIVACY PROTECTION

in our certificateless ring signature scheme, the signer's signature is computed by the key set $\{PK_1, PK_2, \cdots, PK_n\}$. Because of the anonymity of the ring signature, the receiver can not get any specific user's identity information, but can only know that the signature is from a user in the group. In our cloud-assisted body area network public auditing scheme, the data owner calls signing algorithm to generate the integrity checking label and uploads to the cloud server, in the process of tags aggregation and proof verification, cloud server and auditor can't obtain any identity information from the uploaded tags $\{A_{i,1}, A_{i,2}, \ldots, A_{i,n}, B_i\}$ and aggregated tags $(A_1, A_2, \cdots, A_n, M, B)$.

2) BATCH AUDITING

when multiple data blocks are received, the cloud server uses algorithm 5 to aggregate multiple data blocks to generate validation proof. After receiving the verification proof, the auditor checks the integrity of all data blocks. Based on the function of tag aggregation in algorithm 5, the scheme implements batch auditing of multiple data blocks.

3) PUBLICLY VERIFIABLE

when receiving a integrity testing request sent by the user, the third party auditor can complete integrity testing with the cloud server and user through proof generation and proof verification algorithms without additional computational overhead. Therefore, this scheme satisfies the public verifiability.

4) CORRECT STORAGE

when data stored in the cloud server is modified, deleted or damaged, third party auditors can check the integrity of data with our scheme; in addition, due to the reason that the tags generation scheme is unforgeable, so the data stored on the server can be guaranteed to be well-kept. Below, we will prove that our scheme satisfies the non-forgery in random oracle model.

B. NON-FORGERY PROOF

This section lists the theorem 1 and gives a proof.

Theorem 1: in the CLRS scheme, if the co-CDH assumption is hold, then for a polynomial time attacker A, it is difficult to forge a signature.

Proof: suppose A is an attacker who successfully forges the CLRS signature scheme. Given an instance of co-CDH problem: $(P, x \cdot P, Q)$, challenger C can invoke the attacker A's atracking algorithm to output the solution of co-CDH problem. Here we set PK_i as $x \cdot PPK_i \leftarrow x \cdot P$. In this process, the attacker A can check the following quires at any time:

• **quires:**

(1)h quires:

1)C maintains list L_h including tuples $\{A_i, m, PK_1, PK_2, \cdots, PK_n h_i\}$ and initialized as empty.

2)When receiving a quires request $\{A_i, m, PK_1, PK_2, \cdots, PK_n\}$, challenger C checks if tuple $\{A_i, m, PK_1, PK_2, \cdots, PK_n h_i\}$ exists. If exists, challenger C returns h_i to A. 3)Else, challenger C generates a random number $h_i \in Z_q^*$ and returns h_i to A.

(2)H-quires:

1)C maintains the list L_H including of tuples $\{ID_i H_i\}$ and initialized as empty.

2)When receiving a challenge message ID_i, challenger C checks if tuple $\{ID_i H_i\}$ exist. If exits, challenger C returns H_i to A.

3)Else, challenger C generates a random number $h_i \in Z_q^*$ and returns h_i to A.

• **Forgery:**

When challenger sends message m to request signing, attackers invoke the forgery algorithm as the steps below:

1)Chooses $n-1$ elements $A_{i,1}, A_{i,2}, \ldots, A_{i,s-1}, A_{i,s+1,\ldots} A_{i,n} \in G_1$;

2)Chooses two random numbers $o, t \in Z_q^*$, request h-quires and H-quires respectively; computes $A_{i,s} = t \cdot P + o \cdot SK_{i,1} - \sum_{j \neq s}^{n} (h_i \cdot PK_j + A_{i,j}) - h_s \cdot PK_s, B_i = t \cdot Q, O = o \cdot H_i$;

3)Outputs the forging signature $S' = \{A_{i,1}', A_{i,2}', \ldots, A_{i,n}' B', O'\}$.

Due to S is a valid signature on m, so we can get the equations below:

$$e(\sum_{i \neq s}^{n} (h_i \cdot PK_i + A_i), Q)$$

$$= e(\sum_{i \neq s}^{n} (h_i \cdot PK_j + A_i) + h_s \cdot PK_s + A_s, Q)$$

TABLE 4. The computational complexity of the certificateless signature schemes.

	Our scheme	Scheme [17]	Scheme [28]	Scheme [18]
Verification efficiency	$2T_e+dT_m$	$(d+1)T_e+T_p$	$(d+1)\,T_e$	T_e+2dT_m
Signature efficiency	$(d+1)\,T_m+dT_h$	$dT_e+T_H+T_i$	$2dT_m+(d+1)\,T_h$	$(2d+4)\,T_m+4T_h$

(d: the number of users)

$$
\begin{aligned}
&= e(\sum_{i\neq s}^{n}(h_i\cdot PK_j+A_i)+h_s\cdot PK_s+t\cdot P+o\cdot SK_{i,1}\\
&\quad -\sum_{i\neq s}^{n}(h_i\cdot PK_j+A_{i,j})-h_s\cdot PK_s, Q)\\
&= e(t\cdot P+o\cdot SK_{i,1}, Q)\\
&= e((t+o\cdot H_i\cdot msk\cdot P, Q)\\
&= e((t+o\cdot H_i\cdot msk\cdot Q, P)\\
&= e(t\cdot Q+o\cdot H_i\cdot msk\cdot Q, P)\\
&= e(B+O\cdot P_{pub}, P)
\end{aligned}
$$

Challenger can get two valid signatures on message m: $S=\{A_1, A_2, \cdots, A_nB, O\}$ and $S'=\{A_1', A_2', \cdots, A_n', B', O'\}$, $i\in[1,n]$, $i\neq s$, $hi=hi'$. So we can get the equation $B-B'=(h_i-h_i'\cdot x\cdot Q$.

Finally, the challenger outputs $x\cdot Q=(h_i-h_i')^{-1}\cdot(B-B')$ as the solution of co-CDH instance.Through the proof above, we can find that if the scheme can be overcome, then the co-CDH problem is also broken. But the co-CDH assumption is set up, and the contradiction is reached, so our scheme satisfies the unforgability.

From the definition of the theorem 1 we can see that the CLRS scheme is satisfying unforgeability, for the reason that our public auditing scheme in this paper is based on the CLRS ring signature scheme, so the integrity tag of public auditing scheme in this paper cannot be successfully pass the auditor's auditing algorithm when the attacker forges and satisfying the unforgablity in the random oracle model.

IV. THE EFFICIENCY ANALYSIS OF IDENTITY PRIVACY PRESERVING PUBLIC AUDITING SCHEME

The following three experiments (signing and verification stages) are used to compare the efficiency of this scheme with other schemes. The experimental platform is configured as follows: 3.6 GHz processor, 8 G RAM, and the operating system is Windows 7 operating system. We will use the open source cryptography library JPBC to implement this scheme. The selection of elliptic curves is $y^2=x^3+x$, the length of the key is 1024 bits, and the type of bilinear mapping is Tate Paring.

First, we compare the certificateless ring signature scheme CLRS proposed in the paper with the scheme [17], [18], [28], and do two tests: Signature stage and signature verification stage. Table 4 lists the number of cryptographic operations for several schemes, and Figure 4 is the time consumption of testing the signature of [0, 1000] data blocks. It can be found that in several ring signature schemes, the computational complexity of our scheme is the lowest. Figure 5 shows the comparison of signature verification process, because in our scheme, bilinear mapping operation is constant, and the number of bilinear mapping in other schemes will be varying with the change of the number of users, and bilinear mapping operation is the highest computational cost operation, so our signature verification algorithm has efficiency advantage.

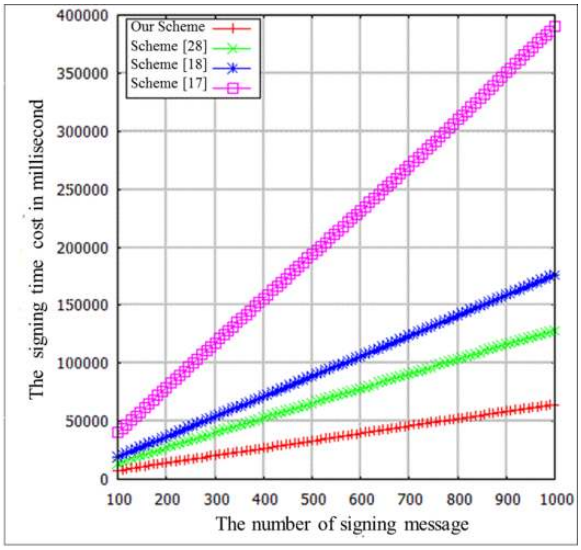

FIGURE 4. The time cost of signing with regard to the number of blocks.

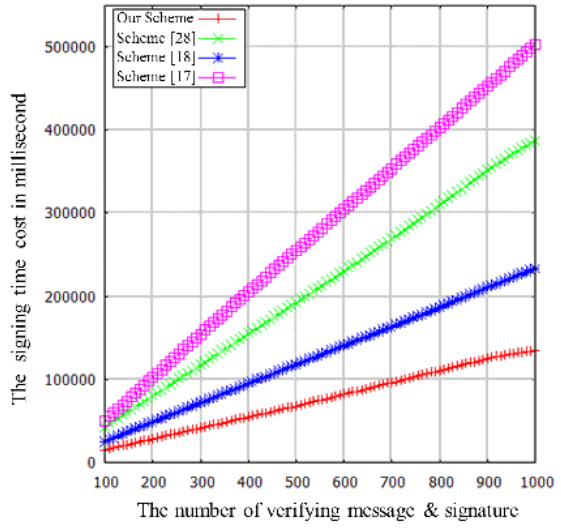

FIGURE 5. The time cost of verifying signature with regard to the number of blocks.

Finally, we compare the auditing phase of several public auditing schemes [14]–[17], which is the most time-consuming stage of the entire auditing process and also is a efficiency bottleneck of the system. As we can see in Figure 6 and table 5, when the tag is aggregated, the computational cost of our scheme is independent of the number of verifying data blocks, only related to the number of members in the ring. After the size of the ring is selected, with increased

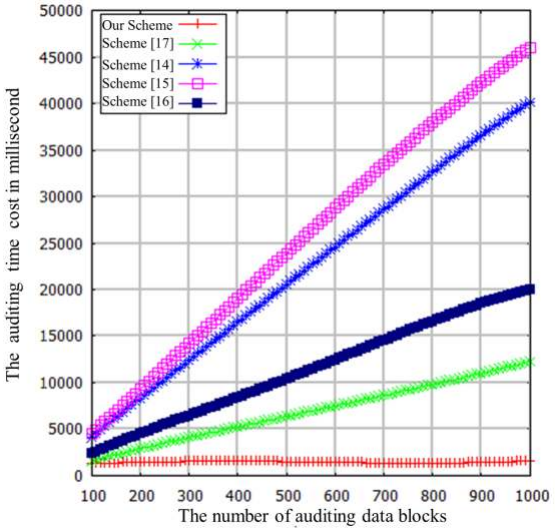

FIGURE 6. The time cost of verifying signature with regard to the number of blocks.

TABLE 5. The time cost of auditing phase with regard to the number of blocks.

Our scheme	Scheme [15]	Scheme [17]	Scheme [16]	Scheme [14]
$2T_e + nT_m$	$(n+1)\,T_e + (n+2)\,T_p$	$(d\ 2)T_e + 2nT_p$	$4T_e + (2n+3)\,T_m$	$nT_e + nT_m$

(n: the number of data blocks, d: the number of usrs)

verification data blocks, our scheme's verification time is a constant; while in [14]–[17], with the increasing of the auditing data blocks, bilinear mapping operation also increases linearly and the cryptographic operation will increase. Through comparison, it is found that our scheme achieves the best efficiency among the comparing schemes.

V. CONCLUSION

In this paper, based on the certificateless ring signature technology, a public auditing scheme for cloud-assisted body area network with identity privacy protection is proposed. This scheme supports the protection of the identity privacy of the data owner in auditing process. This scheme has practical significance considering the needs for the protection of the patient's identity privacy in some wireless body area applications, such as hospitals. Based on the property of the identity privacy protection of the ring signature technology, the auditor can only know that the owner of the data is a member of the anonymous group in the process of auditing. In addition, the scheme is the first public auditing scheme based on certificateless ring signature in cloud-assisted body area network, which is suitable for resource constrained body area network environment. The self-organization of ring signature scheme makes the deployment of the scheme simpler. Through the experiment analysis and comparison, this scheme is also achieving better security and efficiency properties than other similar schemes.

ACKNOWLEDGMENT

The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this article.

REFERENCES

[1] T. G. Zimmerman, "Personal area networks: Near-field intrabody communication," *IBM Syst. J.*, vol. 35, nos. 3–4, pp. 609–617, 1996.
[2] B. Malik and V. R. Singh, "A survey of research in WBAN for biomedical and scientific applications," *Health Technol.*, vol. 3, no. 3, pp. 227–235, Apr. 2013.
[3] A. Samanta and S. Misra, "Energy-efficient and distributed network management cost minimization in opportunistic wireless body area networks," *IEEE Trans. Mobile Comput.*, vol. 17, no. 2, pp. 376–389, Feb. 2018.
[4] R. Sánchez-Montero, C. Camacho-Gómez, P.-L. López-Espí, and S. Salcedo-Sanz, "Optimal design of a planar textile antenna for industrial scientific medical (ISM) 2.4 GHz wireless body area networks (WBAN) with the CRO-SL algorithm," *Sensors*, vol. 18, no. 7, p. 1982, Jun. 2018.
[5] E. Jovanov, A. Milenkovic, C. Otto, P. De Groen, B. Johnson, S. Warren, and G. Taibi, "A WBAN system for ambulatory monitoring of physical activity and health status: Applications and challenges," in *Proc. 27th Annu. Conf. Eng. Med. Biol.*, Jan. 2005, pp. 3810–3813.
[6] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, "Sensor networks for emergency response: Challenges and opportunities," *IEEE Pervas. Comput.*, vol. 3, no. 4, pp. 16–23, Oct. 2004.
[7] F. Axisa, C. Gehin, G. Delhomme, C. Collet, O. Robin, and A. Dittmar, "Wrist ambulatory monitoring system and smart glove for real time emotional, sensorial and physiological analysis," in *Proc. 26th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, vol. 1, Sep. 2004, pp. 2161–2164.
[8] C. W. Mundt, K. N. Montgomery, U. E. Udoh, V. N. Barker, G. C. Thonier, A. M. Tellier, R. D. Ricks, R. B. Darling, Y. D. Cagle, N. A. Cabrol, S. J. Ruoss, J. L. Swain, J. W. Hines, and G. T. A. Kovacs, "A multiparameter wearable physiologic monitoring system for space and terrestrial applications," *IEEE Trans. Inf. Technol. Biomed.*, vol. 9, no. 3, pp. 382–391, Sep. 2005.
[9] G. Fortino, M. Pathan, and G. Di Fatta, "BodyCloud: Integration of cloud computing and body sensor networks," in *Proc. 4th IEEE Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2012, pp. 851–856.
[10] J. Wan, C. Zou, S. Ullah, C.-F. Lai, M. Zhou, and X. Wang, "Cloud-enabled wireless body area networks for pervasive healthcare," *IEEE Netw.*, vol. 27, no. 5, pp. 56–61, Sep. 2013.
[11] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, and C.-H. Youn, "Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 54–61, Jan. 2017.
[12] R. Yu, T. W. C. Mak, R. Zhang, S. H. Wong, Y. Zheng, J. Y. W. Lau, and C. C. Y. Poon, "Smart healthcare: Cloud-enabled body sensor networks," in *Proc. IEEE 14th Int. Conf. Wearable Implant. Body Sensor Netw. (BSN)*, May 2017, pp. 99–102.
[13] L. Wan, G. Han, L. Shu, and N. Feng, "The critical patients localization algorithm using sparse representation for mixed signals in emergency healthcare system," *IEEE Syst. J.*, vol. 12, no. 1, pp. 52–63, Mar. 2018.
[14] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 4, pp. 767–778, Apr. 2017.
[15] J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong, "Privacy-preserving public auditing protocol for low-performance end devices in cloud," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 11, pp. 2572–2583, Nov. 2016.
[16] B. Kang, J. Wang, and D. Shao, "Certificateless public auditing with privacy preserving for cloud-assisted wireless body area networks," *Mobile Inf. Syst.*, vol. 2017, Jul. 2017, Art. no. 2925465.
[17] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," *IEEE Trans. Cloud Comput.*, vol. 2, no. 1, pp. 43–56, Jan. 2014.
[18] Y. Zhang, J. Zeng, W. Li, and H. Zhu, "A certificateless ring signature scheme with high efficiency in the random oracle model," *Math. Problems Eng.*, vol. 2017, Jun. 2017, Art. no. 7696858.
[19] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, to be published.

[20] Z. Yang, W. Wang, Y. Huang, and X. Li, "Privacy-preserving public auditing scheme for data confidentiality and accountability in cloud storage," *Chin. J. Electron.*, vol. 28, no. 1, pp. 179–187, Jan. 2019.
[21] J. Herranz and G. Sáez, "Forking lemmas for ring signature schemes," *J. Manage. Stud.*, vol. 2904, no. 2, pp. 266–279, 2003.
[22] D. Boneh, C. Gentry, and B. Lynn, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in Cryptology*. Berlin, Germany: Springer, 2003, pp. 416–432.
[23] F. Zhang, R. Safavinaini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," *Lect. Notes Comput. Sci.*, vol. 2947, no. 39, pp. 277–290, 2004.
[24] H. Shacham and B. Waters, "Efficient ring signatures without random oracles," in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, 2007, pp. 166–180.
[25] S. Schäge and J. Schwenk, "A CDH-based ring signature scheme with short signatures and public keys," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Tenerife, Canary Islands, Jan. 2010, 2010, pp. 129–142.
[26] J. K. Liu, T. H. Yuen, and J. Zhou, "Forward secure ring signature without random oracles," in *Proc. Int. Conf. Inf. Commun. Secur.* Berlin, Germany: Springer, 2011, pp. 1–14.
[27] K. A. Shim, *An Efficient Ring Signature Scheme From Pairings*. Amsterdam, The Netherlands: Elsevier, 2015.
[28] T. Gao, Q. Wang, X. Wang, and X. Gong, "An anonymous access authentication scheme based on proxy ring signature for CPS-WMNs," *Mobile Inf. Syst.*, vol. 2017, Jun. 2017, Art. no. 4078521.
[29] J. Xu, D. Zhang, L. Liu, and X. Li, "Dynamic authentication for cross-realm SOA-based business processes," *IEEE Trans. Services Comput.*, vol. 5, no. 1, pp. 20–32, Jan. 2012.
[30] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1654–1667, 2020.
[31] U. U. Tariq, H. Ali, L. Liu, J. Panneerselvam, and X. Zhai, "Energy-efficient static task scheduling on VFI-based NoC-HMPSoCs for intelligent edge devices in cyber-physical systems," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, pp. 1–22, Oct. 2019.
[32] D. Miao, L. Liu, R. Xu, J. Panneerselvam, Y. Wu, and W. Xu, "An efficient indexing model for the fog layer of industrial Internet of Things," *IEEE Trans Ind. Informat.*, vol. 14, no. 10, pp. 4487–4496, Oct. 2018.

KAIXIN ZHAO was born in Henan, China, in 1979. He is currently an Associate Professor with the College of Computer Science and Technology, Henan Institute of Technology. His current research interest includes the security of the Internet of Things.

DONG SUN was born in Henan, China, in 1980. He is currently an Associate Professor with the College of Computer Science and Technology, Henan Institute of Technology. His current research interest includes the security of the Internet of Things.

GANG REN was born in Henan, China, in 1978. He received the B.S. and M.S. degrees from Zhengzhou University, Henan, in 2001 and 2005, respectively, and the Ph.D. degree from the Institute of Software, Chinese Academy of Sciences, in 2017. He is currently a Vice Professor with the College of Computer Science and Technology, Henan Institute of Technology, Henan. He is the author of three books, more than 20 articles, and three inventions. Besides, he hosted and participated in three research projects of the National Natural Science Foundation of China. His research interests include big data computing, intelligent computing, deep learning, and parallel computing.

YANG ZHANG was born in Henan, China, in 1990. He received the Ph.D. degree from the Institute of Acoustics, Chinese Academic of Sciences, in 2017. He is currently a Lecturer with the College of Computer Science and Technology, Henan Institute of Technology. His current research interests include cognitive wireless networks, software-defined networks, and underwear acoustic networks.